REMARKS

STATUS OF CLAIMS

Claims 1-26 are pending.

Claims 1-26 are rejected.

Claims 1- 26 are amended.

Thus, claims 1-26 remain pending for reconsideration, which is respectfully requested.

No new matter has been added in this Amendment.

REJECTIONS

The Examiner maintains, from the previous office action, the rejection of claims 1-6 and 16-26 under 35 USC 103(a) as being unpatentable over Yasukawa (US Patent No. 5,999,622), Rhoads (US Patent No. 6,343,138), and Millsted (US Patent No. 6,263,313). Page 3, item 5 of the Office Action.

The Examiner maintains, from the previous office action, the rejection of claims 7-15 under 35 USC 103(a) as being unpatentable over Yasukawa/Rhoads/Millsted in view of Applicants own Admission (ADA). Page 10, item 6, of the Office Action.

Page 2, item 3 is the Response to Arguments, in which the Examiner asserts that the previous arguments have not been persuasive and that the points argued are not recited in the claims.

The independent claims 1, 25 and 26 are amended for clarity to better emphasize the patentably distinguishing features of the present invention. In particular, Yasukawa is directed to ***disc sector-based*** data protection in a file system (Yasukawa, column 1, lines 8-9), whereas the claimed present invention is directed to ***file based*** data protection, as disclosed in page 12, line 2 to page 15, line 6, and FIG. 8 of the present Application.

In contrast to Yasukawa and Millsted, the independent claims 1, 25 and 26, using claim 1 as an example, are amended as follows.

> 1. (CURRENTLY AMENDED) A data management method comprising:
>
> extracting, as a preview sample, a portion of a digital content file to be distributed ~~as sample data~~;
>
> preparing a substantive ~~data unit~~file by encrypting the digital content file;
>
> ~~preparing a sample data unit by~~ embedding user-specific authorization information, containing information for accessing the encrypted digital content file, as invisible information in the extracted preview sample to prepare user-specific-authorization-information-embedded preview sample~~data~~;
>
> ~~preparing a synthesized data unit by~~ synthesizing the substantive ~~data unit~~file and the user-specific-authorization-information-embedded preview sample to prepare a synthesized digital content file ~~data unit having the embedded authorization information~~; and
>
> distributing the synthesized ~~data unit~~digital content file.

In contrast to Yasukawa, Rhoads, and Millsted, the claimed present invention provides that "***user-specific authorization information***" for a protected (typically encrypted) "***substantive file***" is "***embed[ded]***" in a "***preview sample***" of the "***substantive file***." Then, "***preview sample***," which includes embedded use-specific authorization information for accessing the protected "***substantive file***," is "***synthesiz[ed]***" with the "***substantive file***" to prepare "***a synthesized digital content file***."

Therefore, the claims are amended to clarify that the claimed present invention's "***extracting, as a preview sample***" and "***embedding user-specific authorization information,*** containing information for accessing the encrypted digital content file, as invisible information ***in the extracted preview sample to prepare user-specific-authorization-information-embedded preview sample***," is not disclosed or suggested by Yasukawa's disk sector-based data protection of information 36 (which is described in Yasukawa, FIG. 2 and

column 4, line 16 to column 6, line 38).

In other words, Yasukawa, discloses in column 4, lines 16-30 and FIG. 2, that information 36 has an encrypted part 44 and a non-encrypted part 46 which is used to preview the encrypted digital information. However, in contrast to the claimed present invention, Yasukawa discloses that the encrypted part 44 of the information 36 is decrypted by obtaining a decryption key 56 from ***a key distribution center*** and setting the decryption key 56 in the decryption virtual device driver 76 (column 6, lines 30-38). Then, when Yasukawa's application program 60 is invoked, the decryption control interface 70 extracts a volume bitmap table (VBT) 78 showing how the data segments of the information 36 are encrypted and decrypts the data segments of the information 36 using the obtained decryption key 56 (see FIG. 6 of Yasukawa). Therefore, Yasukawa fails to disclose or suggest performing any processing on the non-encrypted part (preview part) 46, which differs from the claimed present invention's ***"embedding user-specific authorization information,*** containing information for accessing the encrypted digital content file, as invisible information ***in the extracted preview sample to prepare user-specific-authorization-information-embedded preview sample***."

Further, Rhoads, which is relied upon by the Examiner for watermarking, does not disclose or suggest the claimed present invention's "***user-specific-authorization-information-embedded preview sample***."

Further, Millsted, which is relied upon by the Examiner for preview samples, does not disclose or suggest the claimed present invention's "***user-specific-authorization-information-embedded preview sample***."

Contrary to the Examiner's suggestion in pages 4-5 of the Office Action, concerning combining Yasukawa with Rhoads and Millsted, a review of Yasukawa, Rhoads, and Millsted, reveals that there is no suggestion, or motivation to one skilled in the art, in Rhoads and Millsted, as well as in Yasukawa, of a desirability to combine and/or modify Rhoads, Millsted and Yasukawa ***to perform any user-specific authorization information processing with respect to a preview sample of information***. In particular, as discussed in the previous After Final Response of May 13, 2004, Millsted is silent on using its Metadata Secure Container (SC) 620, which can include non-encrypted preview information of digital content (column 74, lines 47-67), for providing the claimed present invention's "***user-specific-authorization-information-embedded preview sample***." See, Millsted, column 10, lines 24-33 and column 64, line 61 to column 65, line 18 (which is relied upon by the Examiner in page 5 of the Office

Action) as well as in column 12, lines 21-22, which expressly discloses, "A Watermarking Tool is used to hide data in the Content 113," and not hide data in the Metadata Secure Container 620 as the preview sample. Millsted discloses that the data hid in the Content 113 is data identifying the content owner, the processing date, copy/code play (digital code that defines allowable number of secondary copies and play backs), and other relevant data (column 10, lines 24-33, column 12, lines 21-22 and column 23, lines 57-60). Therefore, Millsted does not disclose or suggest the claimed present invention's, "embedding ***user-specific authorization information*** ... ***in the extracted preview sample to prepare user-specific-authorization-information-embedded preview sample***." In other words, Millsted does not embed, as a watermark, in the Metadata Secure Container 620, "***user-specific authorization information***" to access the Content 113.

Further, in Millsted, as shown in FIGS. 1A, 1B, and 6 and column 28, starting at line 27, the Metadata Secure Container 620 defines data related to Content 113, but does not include the Content 113 itself, so that Millsted does not disclose or suggest the claimed present invention's "***synthesizing*** the substantive ~~data unit~~file and the user-specific-authorization-information-embedded preview sample ***to prepare a synthesized digital content file*** ~~data unit having the embedded authorization information~~." In contrast to the claimed present invention, in FIGS. 1A, 1B, and 6 of Millsted, it is disclosed that the Content Secure Container 113 and the Metadata Secure Container 620 are separate units, the Content 113 is provided to the Content Hosting Sites 111, and the Metadata 620 is provided to the Electronic Digital Content Stores 103 for financial settlement (FIGS. 1A, 1B, and 6, and column 19, line 11 to column 21, line 53).

Further, in contrast to the claimed present invention, Millsted in FIG. 6 provides to an End-User Device 109, a license secure container 660 to access a content 113 item (column 30, lines 3-13). In contrast to Millsted the claimed present invention provides, "***synthesizing*** the substantive ~~data unit~~file and the user-specific-authorization-information-embedded preview sample ***to prepare a synthesized digital content file*** ~~data unit having the embedded authorization information~~."

Therefore, in view of the claim amendments and the remarks, withdrawal of the rejections of pending claims and allowance of pending claims is respectfully requested, because Yasukawa, Rhoads, and Millsted fail to disclose or suggest the claimed present invention as recited in independent claims 1, 25, and 26, using claim 1 as an example, as follows:

> 1. (CURRENTLY AMENDED) A data management method comprising:
>
> extracting, as ***a preview sample, a portion of a digital content file*** to be distributed ~~as sample data~~;
>
> preparing a substantive ~~data unit~~file by encrypting the digital content file;
>
> ~~preparing a sample data unit by~~ ***embedding user-specific authorization information,*** containing information for accessing the encrypted digital content file, as invisible ***information in the extracted preview sample to prepare user-specific-authorization-information-embedded preview sample*** ~~data~~;
>
> ~~preparing a synthesized data unit by~~ ***synthesizing the substantive ~~data unit~~file and the user-specific-authorization-information-embedded preview sample to prepare a synthesized digital content file*** ~~data unit having the embedded authorization information~~; and
>
> ***distributing the synthesized ~~data unit~~digital content file***.

CONCLUSION

There being no further outstanding objections or rejections, it is submitted that the application is in condition for allowance. An early action to that effect is courteously solicited.

Finally, if there are any formal matters remaining after this response, the Examiner is requested to telephone the undersigned to attend to these matters.

Respectfully submitted,
STAAS & HALSEY LLP

Date: 12/16/2004

By: _____
Mehdi D. Sheikerz
Registration No. 41,307

1201 New York Avenue, NW, Suite 700
Washington, D.C. 20005
Telephone: (202) 434-1500
Facsimile: (202) 434-1501